Scottish
Cyber
Coordination
Centre

Daily threat bulletin

27 June 2024

Vulnerabilities

Exploit Attempts Recorded Against New MOVEit Transfer Vulnerability - Patch ASAP!

The Hacker News - 26 June 2024 21:27

A newly disclosed critical security flaw impacting Progress Software MOVEit Transfer is already seeing exploitation attempts in the wild shortly after details of the bug were publicly disclosed. The vulnerability, tracked as CVE-2024-5806 (CVSS score: 9.1), concerns an authentication bypass.

Apple AirPods Bug Allows Eavesdropping

darkreading - 26 June 2024 21:24

The vulnerability affects not only AirPods, but also AirPods Max, Powerbeats Pro, Beats Fit Pro, and all models of AirPods Pro.

Siemens Sicam Vulnerabilities Could Facilitate Attacks on Energy Sector

SecurityWeek - 26 June 2024 10:55

Several vulnerabilities patched recently in Siemens Sicam products could be exploited in attacks aimed at the energy sector. The post Siemens Sicam Vulnerabilities Could Facilitate Attacks on Energy Sector appeared first on SecurityWeek.

CISA Adds Three Known Exploited Vulnerabilities to Catalog

CISA Advisories -

CISA has added three new vulnerabilities to its Known Exploited Vulnerabilities Catalog, based on evidence of active exploitation.CVE-2022-24816 GeoSolutionsGroup JAI-EXT Code Injection Vulnerability, CVE-2022-2586 Linux Kernel Use-After-Free Vulnerability, CVE-2020-13965 Roundcube Webmail Cross-Site Scripting (XSS) Vulnerability. These types of vulnerabilities are frequent attack vectors for malicious cyber actors and pose significant risks to the federal enterprise.

Threat actors and malware

Snowblind malware abuses Android security feature to bypass security

BleepingComputer - 26 June 2024 10:33

A novel Android attack vector from a piece of malware tracked as Snowblind is abusing a security feature to bypass existing anti-tampering protections in apps that handle sensitive user data. [...]

New Caesar Cipher Skimmer targets popular CMS used by e-stores

Security Affairs - 26 June 2024 12:07

A new e-skimmer called Caesar Cipher Skimmer is used to compromise multiple CMS, including WordPress, Magento, and OpenCart. Sucuri researchers discovered a new e-skimmer, called Caesar Cipher Skimmer, that was used in recent weeks to target users of e-stores based on popular CMS, including WordPress, Magento, and OpenCart. Over the past several weeks, the experts […]

‘ChamelGang’ APT Disguises Espionage Activities With Ransomware

darkreading - 26 June 2024 11:00

The China-nexus cyber-threat actor has been operating since at least 2019 and has notched victims in multiple countries.

FakePenny Ransomware, Qilin Ransomware, and More: Hacker’s Playbook Threat Coverage Round-up: June 2024

Security Boulevard - 26 June 2024 18:37

New and updated coverage for ransomware and malware variants, including AI Threat Scenario, GuLoader, DarkGate, MirrorBlast, & Kutaki StealerThe post FakePenny Ransomware, Qilin Ransomware, and More: Hacker’s Playbook Threat Coverage Round-up: June 2024 appeared first on SafeBreach.The post FakePenny Ransomware, Qilin Ransomware, and More: Hacker’s Playbook Threat Coverage Round-up: June 2024 appeared first on Security Boulevard.